United Nations A/68/156

General Assembly

Distr.: General
16 July 2013
English
Original: English/Russian/Spanish

Sixty-eighth session
Item 94 of the preliminary list*
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Contents

		Page
I.	Introduction	2
II.	Replies received from Governments	2
	Cuba	2
	Spain	3
	Ukraine	9
	United Kingdom of Great Britain and Northern Ireland	15

* A/68/50.

13-39735 (E) 020813 020813

Please recycle

I. Introduction

1. On 3 December 2012, the General Assembly adopted resolution 67/27, entitled "Developments in the field of information and telecommunications in the context of international security". In paragraph 3 of the resolution, the General Assembly invited all Member States, taking into account the assessments and recommendations contained in the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201), to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of the concepts mentioned in paragraph 2 of the resolution;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level.

2. Pursuant to that request, on 22 February 2013, a note verbale was sent to Member States inviting them to provide information on the subject. The replies received are contained in section II below. Any additional replies received will be issued as addenda to the present report.

II. Replies received from Governments

Cuba

[Original: Spanish]
[20 May 2013]

The hostile use of telecommunications with the declared or hidden intent of undermining the legal and political order of States is a violation of the internationally recognized norms in this area and can give rise to tensions and situations that are not conducive to international peace and security.

Cuba fully shares the concern expressed in resolution 67/27 regarding the use of information technologies and means of telecommunication that may affect international stability and security and the integrity of States to the detriment of their security in civil and military fields. The resolution also places due emphasis on the need to prevent the use of information resources or technologies for criminal or terrorist purposes.

In this regard, Cuba reiterates its condemnation of the aggressive escalation by successive administrations of the United States of America of their radio and television war against Cuba, which violates the current international rules governing the radio-electric spectrum. This aggression is being perpetrated without regard for the damage that could be caused to international peace and security by creating dangerous situations, including the use of a military aircraft to transmit television signals to the Republic of Cuba without its consent.

Transmissions from aircraft are a violation of regulation 42.4 of the International Telecommunication Union (ITU) Radio Regulations, which prohibits the operation of a broadcasting service by an aircraft station at sea and over the sea.

In 2012, the United States made 192 flights during which, in addition to the illegal transmission of television signals from aircraft into Cuban territory, it simultaneously made illegal FM radio transmissions. These acts caused interference with Cuba's television stations, which are registered in the ITU Master International Frequency Register.

Each week, broadcasters located in United States territory transmit an average of 2,400 hours of radio and television illegally over 30 different television and medium- and short-wave FM radio frequencies. Several of these broadcasters belong to or offer their services to organizations linked with known terrorist elements who live in and act against Cuba from United States territory, broadcasting programmes of incitement to sabotage, political attacks and assassination and committing other forms of radioterrorism.

The illegal radio and television broadcasts against Cuba are intended to promote illegal immigration and encourage and incite to violence, contempt for constitutional order and the perpetration of terrorist acts. Cuba reiterates that the use of information for the clear purpose of subverting the internal order of other States, violating their sovereignty and meddling and interfering in their internal affairs constitutes an illegal act.

These provocative broadcasts against Cuba constitute violations of the international norms governing use of the radio-electronic spectrum contained in the International Radiocommunication Convention, [1] to which the United States Government is a signatory party.

Cuba supported General Assembly resolution 66/24 and will continue to contribute to the peaceful global development of information and telecommunications technologies and their use for the good of all humanity.

Spain

[Original: Spanish]
[29 May 2013]

1. Introduction

Information security is a key aspect of the information society. Technological advances have driven continuous, rapid growth in the capacity to process and store information in multiple formats. Meanwhile, in the area of communications, available bandwidth has increased very significantly and, as a result, huge amounts of information can now be sent and received almost in real time and without the need for particularly complex infrastructures.

While these technological advances improve access to information of all types, they also facilitate the use of and access to information for unlawful purposes,

[1] Translator's note: It appears that the reference should be to the International Telecommunication Convention and the Radio Regulations annexed thereto.

especially the use of information technology and telecommunications systems for hostile or criminal purposes, and even for the commission of terrorist acts or acts of aggression between States or transnational actors.

In recent years, the growing trend in Internet use by criminal organizations and, in particular, by terrorist groups has been confirmed. Such organizations and groups essentially take advantage of two of its characteristics, namely, its global nature and the high degree of anonymity that it can offer.

The development of the information society and information technology must therefore be balanced with the simultaneous development of modern, up-to-date national and international regulations that are appropriate to the new technological environment and capable of responding to the challenges posed by the need to protect information in order to prevent its unlawful use without limiting individuals' rights and freedoms.

2. Misuse of the Internet for terrorist purposes

At present, the main threats arising from the use of the Internet by terrorist organizations are:

(a) Use of the Internet as a weapon, i.e., its use as a means to launch attacks against critical infrastructure information systems or the infrastructure of the Internet itself. Attacks of this kind by common criminals are relatively frequent; however, the attack on Estonia in 2007 made it clear that a State's information infrastructure can also be subject to an attack of this type. The considerable increase in new harmful software in recent years and the "botnets" or networks of "zombie" computers that are used to carry out attacks against information systems are directly related to this type of threat.

(b) Use of the Internet as a medium for other activities, essentially:

- **Communication**. Criminal organizations are increasingly communicating via the Internet instead of using other means, such as fixed or mobile telephones. The tools most frequently used to communicate securely and anonymously over the Internet are electronic mail, instant messaging programmes and online forums.
- **Dissemination of propaganda and terrorism-related materials**. There are currently thousands of websites that incite violence or are related to terrorist activities; this trend has been accentuated with the emergence of Web 2.0 and social networking ("blogs"). Preventing terrorist organizations from using the Internet in this way is quite a complex matter since such websites can be very easily migrated. The phenomenon is transnational since the server that hosts the website may be located in a different country from the one where it is administered while the terrorist organization in question may operate in a third country; where there are no bilateral agreements between these countries, a legal vacuum is created.
- **Recruitment**. The Internet is sometimes used as a means of carrying out recruitment activities, mainly through online forums and instant messaging programmes.

- **Financing**. The Internet also provides opportunities for terrorist organizations to carry out activities aimed at securing funding. The possible involvement of terrorist organizations in Internet fraud, extortion and money-laundering as a means of obtaining financing is of particular interest.

- **Dissemination of training manuals**. Terrorist organizations disseminate manuals on terrorist techniques, the manufacture of explosives and weapons handling via the Internet.

- **Information-gathering to prepare terrorist attacks**. The Internet is a very important source of information that is often used by terrorist organizations to obtain information on the targets of their activities, whether individuals, organizations or infrastructures.

3. Measures taken at the national level to combat Internet use by terrorist organizations

3.1 Legislative measures

Measures adopted by different States include the significant efforts made by Spain in recent years, and particularly in 2007. It has included in its legal system a series of laws relating to information security and the free exercise of the rights and freedoms recognized in the Universal Declaration of Human Rights and the Spanish Constitution. Comprehensive legislation and regulations incorporating both purely national elements and European Union directives have been developed with the aim of meeting these objectives. New information security criteria have been applied based on the premise that in order to achieve a reasonable degree of protection, as well as to maintain the confidentiality of information, it is in most cases essential to preserve the integrity and availability of the information. In particular, the following laws and regulations have been enacted:

- Organization Act No. 5/1992 of 29 October 1992 on regulation of the electronic processing of personal data with the aim of establishing precautionary mechanisms to prevent breaches of privacy resulting from the processing of information; and implementing regulations.

- Organization Act No. 15/1999 of 13 December 1999 on the protection of personal data, which aims to guarantee and protect public freedoms and the fundamental rights of individuals, especially their honour and their personal and family privacy, during the processing of personal data; and implementing regulations.

- Royal Decree-Law No. 14/1999 of 17 September 1999 on electronic signatures, adopted with the aim of encouraging companies, citizens and public authorities to quickly incorporate new technologies for secure electronic communications into their activities, and transposing into Spanish law Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Act No. 59/2003 of 19 December 2003 on electronic signatures updated this framework by incorporating the amendments deemed advisable in light of the experience gained since its entry into force.

- Act No. 11/2002 of 6 May 2002 governing the National Intelligence Centre (CNI), and Royal Decree No. 421/2004 of 12 March 2004, which governs the National Cryptology Centre. By means of these two instruments, the CNI is mandated, among other duties, to coordinate the action of the various Government agencies that use encryption methods and procedures, guarantee the security of information technology in that area and ensure compliance with regulations relating to the protection of classified information.
- Act No. 34/2002 of 11 July 2002 on information society services and electronic commerce, which aims to incorporate into Spanish law Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, on the internal market ("Directive on electronic commerce"). It also partially incorporates Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests since, in accordance with the provisions of that Directive, it governs injunctions against conduct contravening the provisions of the Act.
- General Telecommunications Act No. 32/2003 of 13 November 2003 governing the operation of networks and provision of services in the area of electronic communications.
- Act No. 59/2003 of 19 December 2003 on electronic signatures, already mentioned.
- Act No. 11/2007 of 22 June 2007 on citizens' electronic access to public services, which governs communications between citizens and public authorities using electronic, information and telematic techniques and methods.
- Organization Act No. 10/2007 of 8 October 2007 governing the police database of DNA identifiers. The Act establishes a single database incorporating all files of the State security and law enforcement agencies containing identifiers obtained from DNA analysis carried out as part of a criminal investigation, cadaver identification procedures or missing persons enquiries.
- Act 25/2007 of 18 October 2007 on the preservation of data relating to electronic communications and public communications networks, which is having a positive impact on investigations carried out in this field.
- Royal Decree No. 1720/2007 of 21 December 2007 adopting the implementing regulations for Organization Act No. 15/1999 of 13 December 1999 on the protection of personal data.
- Act No. 56/2007 of 28 December 2007 on measures to promote the information society.
- Criminalization of the following cybercrimes related to the Internet activity of terrorist organizations:
  - Computer sabotage, article 264 of the Penal Code
  - Threats, article 169 and following of the Penal Code
  - Justification or glorification of terrorism, article 578 of the Penal Code

3.2 Other measures

- Creation of specialist police groups to combat use of the Internet by criminal groups.
- Participation in the "*Check the Web*" project developed by the European Police Office (Europol).
- The National Cryptology Centre in the National Intelligence Centre makes a significant daily contribution to the effort to combat cyberattacks. In particular, its Computer Emergency Response Team (CERT) has the capacity to respond to information security incidents. Established in early 2007 as a Spanish governmental body, the CERT participates in the primary international forums, where it shares objectives, ideas and information on cybersecurity.
- Creation of the National Centre for the Protection of Critical Infrastructure
- The Ministry of Defence is taking various steps in the area of cyberdefence. Through the Chiefs of Defence Staff, it participates in the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence, which Spain has been helping to fund since its establishment and to which it provides two experts. The Centre's increasingly important role in the international effort to combat cyberterrorism is illustrated by the recent visit of His Majesty the King, during which he emphasized Spain's commitment to international cybersecurity initiatives.
- NATO is extremely active in cyberdefence activities; it has developed a Concept, adopted a policy and appointed a cyber defence management authority for the alliance.
- The Organization for Security and Co-operation in Europe (OSCE) has established an informal working group on confidence-building measures related to information and communications technologies. The working group's goal is to reduce the potential for cyberattacks while strengthening mutual security through international cooperation, enhancing clarity and transparency and reducing the risks of misperception that could lead to the escalation of conflicts by developing political and military confidence-building measures for the use of information and communications technologies.
- The National Security Scheme sets national security policy for use of the electronic media. It is grounded in basic principles and minimum requirements that allow for adequate protection of information, and all Government departments participate in its work. Its legal basis is a royal decree that will soon be issued pursuant to article 42 of Act No. 11/2007. Spain's Security Strategy identifies the country's primary security threats and risks and sets out a response to them, specifying cyberspace as one of the areas in which action must be taken. This analysis forms the basis for developing response strategies, building capacities and implementing administrative reforms.

National Defence Directive 2012 lists the global threats that Spain must address, stating that cyberattacks are one of the primary risks and that they can be prevented only through a coalition of forces which, in the case of Spain, will be based on NATO and the European Union but will also require the support of other countries and groups of countries that also have a direct interest in monitoring such matters.

This Directive also calls for participation in the promotion of comprehensive cybersecurity management within the framework of the relevant principles of the national cybersecurity strategy.

The Defence Policy Directive, adopted in 2012, also refers to the emergence of cyberspace as a new field of international relations and identifies as a defence priority the strengthening of information- and intelligence-gathering systems in order to support operations such as command and control systems with a view to reducing the risk of cyberattacks.

In January 2011, the Head of the Chiefs of Defence Staff issued a vision of military cyberdefence, which provides guidance for the planning, development and use of the military capacities needed in order to ensure the effective use of cyberspace during military operations.

4. Possible measures that could be taken by the international community to strengthen information security at the global level

Increased dependence on information systems and increased connectivity of critical infrastructures have made cyberspace security essential to the functioning of a modern State. For this reason, cybersecurity should be an intrinsic part of national security planning.

At present, the protection of an international legal framework to meet cybersecurity threats is lacking. Therefore, without prejudice to States' sovereignty in matters related to cybersecurity, there is a need for multilateral cooperation agreements in this area (analogous or similar to the International Convention for the Safety of Life at Sea (SOLAS)) whereby States would undertake to harmonize their legislation with a view to the prosecution of Internet crimes while attempting to ensure, to the extent possible, that anonymity, the absence of legislation and economic interests do not make the Internet the ideal breeding ground for crime and terrorism.

The private sector, and particularly Internet service providers, must be involved in the effort to combat cybercrime. The cooperation of the private sector is essential since most Internet services are in the hands of private companies. The private sector has long dealt with Internet-related threats and its knowledge and experience in this area could be very valuable.

CERTS play a key role in cybersecurity. The establishment of specialized teams and the ongoing training of their members are the first steps that Governments should take in order to ensure cybersecurity. It is also important to establish law enforcement units that specialize in the investigation of crimes committed via the Internet.

Because cybersecurity is a global challenge, international cooperation in improving it is essential and should be strengthened at the policy and operational levels. There should be constant communication between the CERTS of different countries in order to facilitate the sharing of information on attacks within a short response time. Lessons learned and best national and international practices should also be shared.

Other measures include:

- Training citizens and making them aware, at an early age, of the need to pay attention to the security of the information systems that they use. Many types of cybercrime take advantage of (or even depend on) the fact that many Internet users fail to take appropriate precautions in order to make their computers and accounts as secure and impenetrable as possible. User education is therefore essential. Greater awareness of this problem would reduce the number of computers used by cybercriminals in order to carry out their activities, particularly those related to botnets.
- Expediting procedures for international and police cooperation so that criminal offences can be prosecuted rapidly and efficiently, bearing in mind the diffuse nature of the Internet, the volatility of connection records and the legal framework of each country.
- Organizing multinational forums, seminars and conferences in order to enhance the knowledge of experts, share knowledge about the various types of attack and new trends in cyberattacks, assess vulnerability and the impact of potential attacks, share lessons learned and best practices and promote standardized police training in the investigation of cybercrimes.
- Coordinating the efforts of organizations that specialize in specific areas of cybersecurity, such as the Council of Europe and NATO, in order to avoid unnecessary duplication of effort.
- Producing guides and recording good practices, in cooperation with the private sector and civil society, in order to improve cybersecurity.

In conclusion, Spain considers that the international community should adopt whatever information protection measures are deemed necessary, basing its action on an integrated global vision and, if possible, creating a single authority to lay down rules and standards common to all countries, establish a balanced and comprehensive set of specific protection measures and enable the harmonization of the policies and actions of the various national and international organizations involved.

Ukraine

[Original: Russian]
[31 May 2013]

1. General assessment of information security problems

The fields of information security, telecommunications security and cybercrime response are central to the national security of Ukraine. Ensuring the national security of Ukraine, in turn, fosters strengthened international security in a globalizing world.

Globalization, the creation of an information society and the adoption of new information technologies, all of which are occurring worldwide, contribute to the increased importance of information security as a component of national security.

Information security is defined as the degree to which national interests in the field of information are shielded from external and domestic threats.

Accordingly, the following all come under the heading of international threats to information security:

- Unlawful use of information resources
- Unauthorized, destructive activities within automated systems, including those systems used in the management of critical national infrastructure facilities
- Use of cyberspace, related activities or information technologies and resources in a manner that violates fundamental human rights and freedoms or for the purpose of carrying out terrorist, extremist or otherwise criminal acts, including acts of aggression
- Use of information infrastructure to disseminate information that incites animosity and hatred, in general or in a specific country
- Dissemination of information that runs counter to existing national legislation and moral norms and principles
- Use of cyberspace to destabilize society and undermine the economic, political and social system of another State or to spread misinformation designed to distort cultural, ethical and aesthetic values
- Prevention of access to cutting-edge technologies, fostering dependence in the field of information technology in order to gain an advantage and control over foreign cyberspace.

The following globalization-related problem areas should be highlighted: mass or individually targeted informational and psychological manipulation; limitations on consumer access to services based on information and telecommunications technologies; and cybercrime.

According to Ukrainian experts, the following factors may lead to an increased likelihood of the threats described above:

- Low computer literacy on the part of most users of information resources and cyberspace services
- The lack of a common international conceptual framework for information security
- Varied approaches in national legislation to information protection measures designed to establish and update (restore) information infrastructure
- Disparate levels of computerization and information security in different countries
- The danger of linking potentially destructive resources to information and telecommunications systems
- The fact that sources of unauthorized activities in cyberspace may not be clearly identified.

2. National efforts to strengthen information security and support for international cooperation on information security

The main State bodies in Ukraine responsible for information security and its components are the Ministry of Internal Affairs, the Security Service and the State Service for Special Communications and Information Protection. These agencies are actively engaged in regulating the various areas of information security. There is a particular focus on the regulatory and legal framework of the cybernetics component (cybersecurity).

The following legislative provisions on social relations in matters relating to information security are currently in force in Ukraine.

Under article 17 of the Constitution of Ukraine, information security is a crucial State function, along with protecting sovereignty and territorial integrity and maintaining economic security.

In accordance with article 3 of the Information Act of Ukraine, ensuring the information security of Ukraine is one of the main areas of State information policy.

Within the security system of Ukraine as a whole, information security holds a special position, as information relations and processes are component parts of all processes within society and the State. In this context, information security is defined as the status of the information space (environment), which consists of information technologies; information resources and the information relations among the relevant actors, that guarantees the evolution and use of the information space for the benefit of the individual, society and the State.

National security priorities, which are tied to social development interests, determine the main objectives of information security. These objectives are as follows:

- Ensuring Ukraine's national information sovereignty as information flows become increasingly globalized and other countries compete for ascendancy in the field of information
- Creating an information environment that supports the cultural, moral and intellectual development of the individual and society as a whole
- Maintaining the informational resources of Ukraine at levels sufficient to guarantee the sustainable functioning and development of the individual, society and the State
- Protecting the information of natural and legal persons and the State from external and domestic information threats, which includes responding to computer crimes
- Ensuring the validity and enforcement of the rights of information stakeholders in Ukraine to create and use national information resources, information technologies and information infrastructure.

To strengthen information security, a regulatory and legal framework and professional training system are being implemented, and there is coordination of the activities of State agencies responsible for information security. This coordination includes cooperation with the Computer Emergency Response Team of Ukraine

(CERT-UA), and the Forum of Incident Response and Security Teams (FIRST), an internationally accredited organization.

Under Ukrainian law, CERT-UA operates as part of the State Service for Special Communications and Information Protection, coordinating the work of enterprises, institutions and organizations, regardless of ownership structure, in order to prevent, analyse and respond to the consequences of unauthorized actions that target State information resources in information and telecommunications systems.

Moreover, CERT-UA cooperates with the relevant foreign and international bodies and organizations, and the Team's obligations to its foreign counterparts (full membership in FIRST and membership in the International Multilateral Partnership Against Cyber Threats of the International Telecommunication Union) encourage international information security cooperation.

Under the Act of Ukraine on amendments to the Act ratifying the Convention on Cybercrime, the Ministry for Internal Affairs is the body authorized to establish and oversee the 24-hour network of points of contact for emergency assistance with computer systems and data crime investigation; prosecution of individuals accused of such crimes; and electronic evidence-gathering.

The relevant unit, which manages the 24-hour cybercrime response network of the Anti-Cybercrime Division, operates within the Ministry for Internal Affairs and is responsible for implementing the relevant activities and operations, including the following:

- Countering distributed denial-of-service attacks
- Combating criminal offences committed using payment cards or their account data
- Combating unauthorized interference in the operations of "client-bank" remote banking services
- Countering dissemination of illegal Internet content (in violation of copyright)
- Countering Internet dissemination of pornography, including child pornography
- Countering telecommunications offences
- Countering offences related to unauthorized access to satellite data transmission networks
- Countering financial and other types of fraud perpetrated over the Internet
- Countering criminal and other e-commerce offences
- Managing the cybercrime response operations of the 24-hour network of points of contact.

Efforts are currently being made to update national information security legislation in order to develop a regulatory and legal framework that is harmonized with international norms.

A draft law on cybersecurity is now being drafted in Ukraine, in accordance with Presidential Decree No. 1119 of 10 December 2010 on the decision of

17 November 2010 of the National Security and Defence Council of Ukraine on challenges and threats to the national security of Ukraine in 2011.

The following national policy areas may receive greater attention under existing regulatory and legal acts:

(1) Presidential Decree No. 1119 of 10 December 2012 on the decision of the National Security and Defence Council of 17 November 2010 on challenges and threats to the national security of Ukraine in 2011 (paragraph 4); Presidential Decree No. 388 of 8 June 2012 on the decision of the National Security and Defence Council of 25 May 2012 on activities to strengthen counter-terrorism in Ukraine (paragraph 1); Presidential Decree No. 389 of 8 June 2012 on the decision of the National Security and Defence Council of 8 June 2012 on the updated National Security Strategy Council (subparagraphs 3.1.1, 3.3 and 4.3); and Presidential Decree No. 390 of 8 June 2012 on the decision of the National Security and Defence Council of 8 June 2012 on the updated Military Doctrine of Ukraine (subparagraphs 7 and 19), contain the following objectives:

- Setting up a national cybersecurity system
- Setting up a unified nationwide system to combat cybercrime
- Drafting and approving a register of critical national security and defence sites that are cyberattack protection priorities
- Drafting and submitting to the Parliament a draft law on national cybersecurity
- Defining cybersecurity as one of the central threats to international stability and Ukrainian national security
- Approving, as a strategic goal and primary national security policy objective, the preparation of national standards and technical regulations for information and communications technologies use and their harmonization with the relevant standards of European Union member States
- Defining the term "cyberterrorism"
- Establishing an effective mechanism in Ukraine for responding to the newest national security threats (phenomena and trends that could, under certain conditions, threaten national interests) related to information technology use in a globalizing world, especially "cyberthreats"
- Analyzing cyberattacks that target nuclear and chemical industry facilities, military-industrial facilities and other potentially hazardous sites in a show of military force against Ukraine that could lead to military conflict;

(2) Regulatory and legal acts of the Cabinet of Ministers: Order No. 720-r of 22 August 2012 approving the Annual National Programme of Ukraine-North Atlantic Treaty Organization (NATO) Cooperation for 2012 as well as Instruction No. 24066/1/1-12 of 15 June 2012 under the aforementioned Decision of the National Security and Defence Council, implemented under Presidential Decree No, 388 of 8 June 2012, which also provides for the elaboration of a legislative act on cybersecurity;

(3) The Parliament of Ukraine is considering draft laws to amend some acts on national cybersecurity. These draft laws provide, inter alia, for the use in national legislation of such concepts as "State cybersecurity", "critical infrastructure sites",

"critical information infrastructure sites" and "cyberspace", and for the definition of the primary cyberthreats to national security, the main areas of State policy and the tasks of the entities responsible for national security in this field.

3. Adoption of international frameworks to strengthen global information and telecommunications systems security

Ukraine has a regulatory and legal framework to protect information in information and telecommunications systems whose principles and approaches to structuring protection are harmonized with International Organization for Standardization 15408/Common Criteria for Information Technology Security Evaluation.

Given that computer crime has escalated beyond national borders and grown into an international phenomenon, Ukraine cooperates with foreign law enforcement agencies on an ongoing basis.

In addition, under projects and programmes with the Organization for Security and Co-operation in Europe, the Parliamentary Assembly of the Council of Europe, the Council of Europe and the NATO Partnership for Peace, and in the context of bilateral agreements, Ukraine is working to secure international information security.

4. Possible measures that could be taken by the international community to strengthen information security at the global level

Owing to the transnational nature of computer crime, it may be time to draft a set of international principles to strengthen information and telecommunications network security and international security policy overall, and to enhance ways, means and resources for information security threat detection, assessment and forecasting.

One of the main areas of global information security involves the drafting and adoption of international legal instruments to eliminate imprecise information security terminology. An important aspect of this would be to determine the international legal status of cyberspace and to enshrine, in regulatory and legal instruments, States' jurisdictions with regard to the national components of this space (comparable to States' air space and territorial waters) and the further regulation of issues related to cyberwar, cyberaggression, and so on.

Another key aspect of standard-setting in the field would be the adoption of a unified concept of cybercrime, as well as a clear classification of the relevant offences.

Other measures that the international community could take to strengthen global information security might include harmonization of the regulatory and legal framework for information protection; development of agreed criteria and methods for assessing the effectiveness of information security systems and resources; mutual recognition of information security certificates; and expanded cooperation in addressing research, technical and legal information security issues. At the same time, stepping up cooperation among national law enforcement agencies to prevent, suppress and prosecute computer crimes is crucial to successful cooperation.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[16 May 2013]

The United Kingdom of Great Britain and Northern Ireland welcomes the opportunity to respond to General Assembly resolution 67/27 entitled "Developments in the field of information and telecommunications in the context of international security".

General appreciation of the issues of information security

The United Kingdom will use its preferred terminology of "cybersecurity" and related concepts in the present submission, denoting efforts aimed at the preservation of the confidentiality, availability and integrity of information in cyberspace. The term "information security" is often used by business and standards organizations to mean the same thing, and the term is also accepted by the United Kingdom with this specific meaning. There is scope for potential confusion in the use of the term "information security" in that it is used by some countries and organizations as part of a doctrine that regards information itself as a threat against which additional protection is needed. The United Kingdom does not recognize the validity of the term "information security" when used in this context, since it could be employed in attempts to legitimize further controls on freedom of expression beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Cyberspace is a domain of great opportunity but also of actual and potential threat. Over two billion people are now connected to cyberspace through the Internet, with that number set to grow further as mobile technologies allow developing countries to take advantage of its enormous benefits at lower costs. The Internet provides an engine for economic growth, opens up access to education, strengthens human interaction and understanding, breaks down cultural and geographic barriers, allows services to be delivered online and strengthens democracy by holding Governments accountable to its citizens in new and dynamic ways. For example:

- Internet-based activity already accounts for eight per cent of the gross domestic product of the United Kingdom. Ensuring that businesses and customers feel secure about doing business in cyberspace is crucial to economic growth.
- The United Kingdom introduced an e-petitions service in 2011, allowing anyone to open or sign a petition on an issue for which Government has responsibility. All petitions attracting 100,000 signatures or more are considered for debate in Parliament. In its first year, over 15,600 petitions were opened, of which 10 passed the 100,000 threshold. All of these have either been debated or scheduled for parliamentary debate.

The United Kingdom, like many countries, relies on cyberspace in many areas of critical national services, such as energy, finance and transport. Significant failures in these services, whether accidental or as the result of a deliberate intrusion, could cause severe disruption, economic damage or loss of life.

The threat landscape is complicated and dynamic. Systems of the Government of the United Kingdom, along with those of business and private individuals, are subjected to attempted intrusions on a daily basis. Motives range from political and industrial espionage, cybercrime, disruption or control of networks or denial of service. Threat actors range from nation States, State proxies, non-State actors, and organized criminal gangs through to opportunistic individuals. The interconnected nature of cyberspace means that disruptive activities against one system may cause unintended and unpredictable effects in other systems. Attempts to counter these threats are hampered by the difficulty in reliably attributing a cyber incident to a particular source, the potential for the perpetrators to masquerade as others, immature understanding of acceptable State behaviour in cyberspace, the lack of resilience in the cyber infrastructure in some countries and the absence of harmonized international approaches to detect, pursue and prosecute cybercriminals.

All elements of society have a role and a duty in combating these threats. It is for Governments to lead international efforts to improve understandings over acceptable State behaviour and in tackling cybercrime but, given that the majority of the infrastructure of cyberspace is owned and operated by private companies, their participation in this debate is crucial. The United Kingdom believes that improved cybersecurity must not come at the expense of the economic and social benefits that cyberspace brings. It is particularly important to ensure that efforts to increase cybersecurity are not misused to impose further restrictions on freedom of expression beyond those permitted in international agreements. In this regard, the role of civil society organizations is particularly important.

Efforts taken at the national level to strengthen information security and promote international cooperation in this field

National approaches

The United Kingdom's national security strategy, published in 2010 identified cyberattacks as one of four "tier 1" threats, alongside an international military crisis, major accidents or natural hazards and terrorist attacks. In November 2011, the United Kingdom published an updated cybersecurity strategy which sets out a vision to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society. The achievement of this strategy is supported by four objectives:

- To tackle cybercrime and be one of the most secure places in the world to do business in cyberspace
- To be more resilient to cyberattacks and better able to protect our interests in cyberspace
- To help shape an open, stable and vibrant cyberspace that the public of the United Kingdom can use safely and that supports open societies
- To have the cross-cutting knowledge, skills and capability it needs to underpin all our cybersecurity objectives

To underpin the achievement of these objectives, the Government of the United Kingdom allocated £650 million of additional expenditure to be used in a four-year programme intended to transform the response to cyberthreats.

The United Kingdom has invested in new and unique capabilities to protect its core networks and services and to deepen its understanding of the threat it faces. In turn, this enhanced knowledge allows it to better prioritize and direct defensive efforts. Under the auspices of the Ministry of Defence of the United Kingdom, it has established a tri-service unit to develop new tactics, techniques and plans to deliver military capabilities in response to sophisticated threats. The Government works closely with victims of disruptive cyberactivity and the results of that work allow it to provide advice to industry to improve their cybersecurity measures. In terms of its own networks, it is developing a new security model for the sharing of services, including more sophisticated employee authentication, better policing of compliance and greater network resilience.

The Government of the United Kingdom has invested in strengthening law enforcement and prosecutorial capabilities to prevent, disrupt and investigate cybercrimes and bring those responsible to justice. The Police Central e-Crime Unit has tripled in size, three regional cyberpolicing teams have been established and training on combating cybercrime for mainstream police officers has been designed. The Serious Organized Crime Agency will merge with the Police Central e-Crime Unit later in 2013 to form the National Cybercrime Unit of the National Crime Agency, a further step towards improving the law enforcement capability of the United Kingdom against cybercrime.

United Kingdom industry is the biggest victim of cybercrime, including the widespread theft of intellectual property. The Government works with industry and academia to promote awareness of the need to address cyberthreats and, in 2012, it produced a guidance document for industry chief executives that set out how senior executives should adopt strategies to protect their most valuable information assets. The Government has also successfully completed a pilot information-sharing initiative to provide a trusted environment for organizations to share information on current threats and managing incidents. This included around 160 companies in the defence, finance, pharmaceuticals, energy and telecommunications sectors.

In conjunction with industry, the Government of the United Kingdom has been active in raising awareness of the threat among industry and the public so that they take the often simple steps to protect themselves and demand better security in cyberproducts and services. These initiatives have included "Get Safe Online Week" (run with the European Union and Canada), targeted campaigns on online fraud delivered by the National Fraud Authority and a "Devils in your details" campaign in 2012.

The United Kingdom is investing in skills and research so that we have the capability to keep pace with this problem in the future. The first eight United Kingdom universities to have conducted research in the field of cybersecurity have been given the status of academic centres of excellence in cybersecurity research. Interactive learning materials are being developed for younger students and a technical apprenticeship scheme has been launched to identify and develop talent in school and university students. In order to ensure that those working in the field of cybersecurity receive the right education and training, a scheme on certification for information assurance professionals will help Government and industry to recruit cybersecurity professionals with the right skills at the right level to the right jobs.

International approaches

The United Kingdom has been at the forefront of international efforts to improve the transparency, predictability and stability of cyberspace. In November 2011, the United Kingdom hosted the first International Conference on Cyberspace, which brought together representatives from over 60 countries and from business and civil society organizations to discuss ways of expanding the economic and social benefits of cyberspace, cooperation on tackling cybercrime, safe and reliable access to the Internet and international security. The momentum generated by the event was taken forward at the 2012 Conference, held in Budapest, and planning is already under way for the 2013 Conference, to take place in Seoul.

The United Kingdom is an active member of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Conext of International Security and of the informal working group of the Organization for Security and Cooperation in Europe (OSCE) on establishing confidence-building measures for cyberspace.

In October 2012, the United Kingdom announced an initiative to set up a centre for global cybersecurity capacity-building, with funding of £2 million per year, to include various multilateral and bilateral initiatives. The centre will offer independent advice and expertise to other countries on how to build more secure and resilient national infrastructures and become a focal point for world class research and international collaboration on this vital issue.

In order to further international efforts to tackle international cybercrime, the United Kingdom continues to promote the Convention on Cybercrime and its principles as the most effective instrument in this field. The Serious Organized Crime Agency continues to lead with international partners on the global representation of law enforcement issues to the Internet Corporation for Assigned Names and Numbers.

Relevant international concepts aimed at strengthening the security of global information and telecommunications systems

The paramount concept is that of the application of international law and the existing norms of behaviour that govern relations between and among States. The United Kingdom firmly believes that these principles apply with equal force to cyberspace and an unambiguous affirmation by States that their activities in cyberspace will be governed by these laws and norms would lay the foundations for a more peaceful, predictable and secure cyberspace.

In this regard, cyberspace presents particular challenges, for example, the difficulties in the reliable attribution of activities, assessment of intent and the role of non-State actors. The United Kingdom would welcome international discussions on how to apply international law and norms of State behaviour in this context.

The United Kingdom does not believe that attempts to conclude comprehensive multilateral treaties, codes of conduct or similar instruments would make a positive contribution to enhanced cybersecurity for the foreseeable future. The complex and comprehensive nature of any binding agreement across the entirety of a cyberspace that is evolving at "net speed" means that it could not be effective or command widespread support without many years, possibly decades, of painstaking work on norms of behaviour and confidence-building measures to build

up the necessary understanding and trust among signatories and to ensure that they can be reliably held to account for their adherence to their commitments. Experience in concluding these agreements on other subjects shows that they can be meaningful and effective only as the culmination of diplomatic attempts to develop shared understandings and approaches, not as their starting point. The United Kingdom believes that the efforts of the international community should be focused on developing common understandings on international law and norms rather than negotiating binding instruments that would only lead to the partial and premature imposition of an approach to a domain that is currently too immature to support it.

Possible measures that could be taken by the international community to strengthen information security at the global level

The borderless nature of cyberspace provides a particular imperative for States to enhance bilateral, regional and multilateral cooperation to develop common responses to common threats. In the view of the United Kingdom, the measures that could make the most significant contribution at this stage are:

(a) Continuing discussions among States to develop a normative framework of acceptable State behaviour based on existing principles of international law and customary international norms;

(b) The development of confidence building measures for cyberspace aimed at increasing the transparency and predictability of State behaviour, thus reducing the risk of misperception or unintended escalation of incidents;

(c) The establishment of computer emergency response teams by States as a focus for incident-handling and information-sharing, supplemented by notification of key points of contact and reliable crisis communications mechanisms;

(d) The development of joint exercises to test joint incident-handling and communications procedures;

(e) The development of harmonized legal approaches to tackle cybercrime;

(f) Enhanced dialogue with business and civil society representatives to ensure coordinated and prioritized approaches in a domain that is largely owned and operated by the private sector;

(g) Commitments by States with more mature cybersecurity capabilities to support capacity-building for other States.